ڈیجیٹل سیکورٹی

انتساب: شہید فدائی بابر مجید بلوچ

ہکّل پبلیکیشنز

BALOCH LIBERATION ARMY
B.L.A
STRUGGLE TILL VICTORY

ڈیجیٹل سیکورٹی

اشاعت: دسمبر 2021

ہکل پبلیکیشنز

بلوچ لبریشن آرمی

ڈیجیٹل سیکورٹی

موبائل فون اور ڈیجیٹل وسائل پر انحصار آج زندگی کا ایک اہم حصہ بن چکا ہے۔ ایک سیاسی کارکن کو روزمرہ کے واقعات اور سیاسی سرگرمیوں کی نگرانی کرنے اور خاص طور پر دشمن سے متعلق تمام معلومات سے باخبر رہنے کیلئے آن لائن وسائل سے بہت مدد مل سکتی ہے۔ تاہم، یہی آلات آپ کو ریاستی ہیکرز اور حکام کی طرف سے خطرے میں بھی ڈال سکتے ہیں۔ ایک آزادی پسند جہدکار ہونے کے ناطے آپ ہمیشہ خطرے میں رہتے ہیں۔ خود کو آن لائن حملوں اور نگرانی کی کوششوں سے بچانے کے لیئے، جدید ترین ڈیجیٹل سیکیورٹی طریقہ کاروں کو اپنانے کی ضرورت ہوتی ہے۔

یہ دستاویز کچھ بنیادی ڈیجیٹل حفاظتی تدابیر سے متعلق معلومات اور طریقہ کار فراہم کریگی۔ جس پر درست انداز میں عملدرآمد کرنے سے آپکو ایسے نقصاندہ حملوں سے بچنے میں مدد مل سکتی ہے، جو آپکی اور آپکے جہدکار ساتھیوں کی جان کو خطرے میں ڈال سکتی ہیں۔

کچھ بنیادی اقدامات:

- **اولین اور اہم ترین، اپنی آن لائن موجودگی کو محدود رکھیں:**

انٹرنیٹ یا موبائل فون محض اس صورت استعمال میں لائیں، جب انکی ضرورت ہو۔ بلاضرورت آن لائن رہنے سے حددرجہ اجتناب کریں۔ یہ دیکھا گیا ہے کہ بہت سے بلوچ آزادی پسند جہدکاروں کی آن لائن موجودگی ضرورت سے بہت زیادہ ہے۔ ایک بار جب کسی اکاؤنٹ کو تسلسل کے ساتھ آن لائن دیکھا جاتا ہے، تو اسکے خلاف کاروائی کا خطرہ بڑھ جاتا ہے۔ نگرانی سے بچنے کا سب سے آسان طریقہ یہ ہے کہ ضرورت سے زیادہ آن لائن رہنے سے حددرجہ گریز کیا جائے۔ یہ سادہ اور بنیادی نکتہ انتہائی اہم ہے۔

- **اپنے موبائل آلات کو اپ ٹو ڈیٹ رکھیں:**

ایپل اور اینڈرائیڈ آج کے دور کے دو اہم آپریٹنگ سسٹمز ہیں۔ انکے پاس جدید ترین سافٹ ویئر موجود ہیں۔ تاہم، ان کے سسٹمز کی پیچیدگی ہمیشہ ہیکرز کیلئے کوئی نا کوئی گھسنے کا موقع چھوڑ دیتی ہے۔ تاہم، اچھی بات یہ ہے کہ یہ کمپنیاں اس طرح کی خلاف ورزیوں کی مسلسل نگرانی کرتی ہیں اور باقاعدگی سے سیکیورٹی اپ ڈیٹس بھی جاری کرتی ہیں۔ لہٰذا، یہ بہت ضروری ہے کہ آپ اپنے آلے کو جدید ترین آپریٹنگ سسٹم پر اپ ڈیٹ رکھیں۔ آپ ہمیشہ اپنے ایپلیکیشنز کو آٹو اپڈیٹ پر رکھیں اور یقینی بنائیں کہ وہ اپ ٹو ڈیٹ ہیں۔ یہ بھی یقینی بنائیں کہ آپ کا موبائل پاسورڈ 6 حروف سے زیادہ ہے، محض 4 حروف پر مشتمل پاسورڈ کو کریک کرنا بہت آسان ہوتا ہے۔

- یک رسائی پاس کوڈ استعمال کریں۔

ان دنوں بہت سے فون چہرے کی شناخت اور ٹچ آئیڈ ینٹی کے ذریعے بائیو میٹرک ان لاک کے ساتھ آتے ہیں۔ کبھی بھی ایک پاس کوڈ بائیو میٹرک لاگ ان کیلئے استعمال نہ کریں۔ بالفرض، اگر آپ دشمن کی حراست میں آتے ہیں تو انہیں آپ کے جسم تک رسائی حاصل ہو جاتی ہے، وہ طاقت کے ذریعے آپ کے آلے میں لاگ ان کرنے کی صلاحیت رکھیں گے۔ لہٰذا پاس کوڈ استعمال کریں، پاس کوڈ کا فائدہ یہ ہوتا ہے کہ آپ کا فون آپ کی انگلی یا چہرے سے کھولا نہیں جاسکتا ہے۔

- پاس ورڈز کے بارے میں ہوشیار رہیں:

مضبوط پاس ورڈز آپ کے اکاؤنٹس تک غیر مجاز رسائی کے خلاف دفاع کی پہلی لائن ہوتی ہیں۔ ہمیشہ پیچیدہ اور منفرد پاس ورڈ استعمال کریں، جن کا آسانی سے اندازہ نہ لگایا جا سکے۔ بڑے A اور چھوٹے a دونوں حروف کا مجموعہ استعمال کریں اور پاس ورڈ میں خصوصی حروف *£@ اور نمبر وغیرہ شامل کریں۔ Balochistan 123 جیسا پاس ورڈ کمزور ہے، اسے استعمال نہیں کرنا چاہیئے، دوسری طرف **PaR0om984!!** جیسے پاس ورڈ کا اندازہ لگانا بہت مشکل ہوتا ہے۔ مختلف اکاؤنٹس کے لیے مختلف پاس ورڈ استعمال کریں اور کبھی بھی اپنے پاس ورڈز مشترک نہ رکھیں۔ ہر چند ماہ بعد اپنے پاس ورڈز تبدیل کرنا بھی ایک اچھا عمل ہے۔

- اپنے فون کو بند رکھیں:

اپنی سیٹنگ کو تبدیل کریں تاکہ آپ کا فون سونے کے فوراً بعد بند ہو جائے اور پاور بٹن دبانے کے فوراً بعد لاک ہو جائے۔

- اپنی نوٹیفکیشن چھپائیں:

معلومات کی مقدار کو محدود رکھیں تاکہ کوئی بھی آپ کے پیغامات نہیں دیکھ سکے۔ پیغام رسانی ایپ کی اطلاعات کو پیغامات کا مکمل مواد دکھانے سے روکیں۔

- اپنے تمام آلات کو(ENCRYPT) کریں:

یہ قانون نافذ کرنے والے اداروں یا ہیکرز کے لیے آپ کے آلات پر ڈیٹا تک رسائی کو بہت مشکل بنا دیتا ہے۔ آئی فونز پہلے ہی انکرپٹڈ ہیں۔ اینڈرائیڈ فونز نہیں ہیں، اس لیے آپ کو سیکیورٹی سیٹنگز میں جانا چاہیئے اور انکرپشن کو فعال کرنا چاہیئے۔ میک کمپیوٹرز پر، سسٹم کی ترجیحات میں جائیں، پھر سیکیورٹی اور پرائیویسی، اور `File Vault` کو آن کریں۔ ونڈوز پر، آپ کو اپنی ڈرائیو کو خفیہ کرنے کے لیے بٹ لاکر ایپلیکیشن کا استعمال کرنا چاہیے۔

- ہمیشہ VPN استعمال کریں:

آن لائن براؤزنگ کے لیے یہ بہت ضروری ہے کہ آپ ہمیشہ VPN کا استعمال کریں، اس ضمن میں کچھ اچھے براوزر Psiphon اور Aloha Browser موجود ہیں۔ VPN آپ کی انٹرنیٹ سرگرمی کو گمنام رکھنے میں مدد کرے گی اور آپ کے آن لائن ہونے پر آپ کو ایک نجی، محفوظ کنکشن فراہم کرے گا۔

- ٹور نیٹ ورک کا استعمال کریں(Tor Network):

VPNs کے علاوہ آپ کو آن لائن براؤزنگ کے لیے TOR نیٹ ورک کا براؤزر بھی استعمال کرنا چاہیے، جب آپ ٹور نیٹ ورک سے منسلک ہوتے ہیں، تو کوئی بھی آپکے انٹرنیٹ سرگرمی یا ڈیٹا کو ٹریس نہیں کرسکتا کیونکہ آپکا ڈیٹا متعدد بار انکرپٹ ہوتا ہے۔ ایک اور اچھا براؤزر Brave ہے، جو آپ کی شناخت کی بھی حفاظت کرتا ہے۔

- ہمیشہ نجی موڈ میں براؤز کریں(private mode):

انٹرنیٹ براؤز کرتے وقت ہمیشہ پرائیویٹ موڈ استعمال کریں۔اس موڈ پر براوزر یہ ڈیٹا نہیں رکھتا کہ آپ کن ویب سائٹس پر جارہے ہیں۔ یہ خاص طور پر اس وقت مفید ہے، جب آپ کا موبائل دشمن قوتوں کے ہاتھ لگ جائے یا آپ کو سیکیورٹی چیک پوسٹ پر روکا جائے اور آپ کا موبائل چیک کیا جائے۔

- روابط کے لیے سگنل ایپلیکیشن استعمال کریں:

زیادہ تر جدید ترین میسجنگ سافٹ ویئر اینڈ ٹو اینڈ انکرپٹڈ ہیں، یعنی آپ اور میسج وصول کنندہ کے علاوہ کوئی اور آپ کے پیغامات نہیں پڑھ سکتا۔ تاہم سیکورٹی ماہرین ہمیشہ سگنل استعمال کرنے کا مشورہ دیتے ہیں۔ بات چیت کے لیے کبھی بھی عام SMS کا استعمال نہ کریں، یہ بہت آسانی سے ریاستی حکام کی طرف سے ٹریس کیا جاسکتا ہے۔

- ای میلز کے لیے Proton Mail استعمال کریں:

سگنل کی طرح، پروٹون میل بھی اینڈ ٹو اینڈ انکرپٹڈ ہے۔ یہ ای میلز بھیجنے اور وصول کرنے کا ایک پلیٹ فارم ہے اور عام جی میل/آؤٹ لک اکاؤنٹس سے زیادہ محفوظ ہے۔

- ایپ کی Permissions چیک کریں:

کیا آپ کے ڈاؤن لوڈ کردہ گیم کو آپ کے مقام، تصاویر یا رابطوں تک رسائی کی ضرورت ہے؟ بہت سی ایپس اور سائٹس کو کام کرنے کے لیے ان چیزوں کو جاننے کی ضرورت نہیں ہے، پھر بھی وہ انسٹالیشن کے دوران ڈیفالٹ کے ذریعے ان کی درخواست کرتی ہیں۔ اپنی ترتیبات پر ایک نظر ڈالیں، اور ان اجازتوں کو بند کردیں، خاص طور پر اپنا مقام۔

- اپنے موبائل پر ایپس کی تعداد کو محدود کریں:

صرف وہی موبائل ایپس انسٹال کریں، جن کی واقعی ضرورت ہے۔ ایپس آپ کے ڈیٹا تک رسائی حاصل کرسکتی ہیں اور بہت سے دوست سوچتے ہیں کہ اگر کوئی "ایپ" ایپ اسٹور یا گوگل پلے کے ذریعے ڈاؤن لوڈ کیا گیا ہے تو اس کا استعمال محفوظ ہوگا، ایسا نہیں ہے کوئی بھی ایپ بنا کر اسے گوگل پلے میں شامل کرسکتا ہے، یہ پھر کسی خاص جغرافیائی علاقے یا معاشرے کے طبقے کو نشانہ بنا سکتا ہے اور آپکے موبائل کے ذریعے معلومات نکال سکتا ہے۔

- **اپنے فون پر کم سے کم ڈیٹا رکھیں:**

یہ دیکھا گیا ہے کہ بہت سے ساتھی تنظیم کے دیگر ساتھیوں کی تصاویر اور ویڈیوز کی شکل میں بہت سا ڈیٹا اپنے پاس رکھتے ہیں۔ یہ انتہائی خطرناک اور انتہائی غیر ذمہ دارانہ عمل ہے۔ اگر یہ موبائل دشمن کے ہاتھ لگ جاتا ہے، تو وہ تنظیم کے دیگر ارکان کے بارے میں معلومات بآسانی ٹریک کر سکتے ہیں۔ ہمیشہ خود سے ایک سوال پوچھیں کہ اگر آپ کا موبائل فون آپکے دشمن کے ہاتھ میں ہے تو کیا ہوگا؟ ہم نہ صرف اپنی حفاظت کا خیال رکھیں بلکہ تنظیم کے دیگر ارکان کی حفاظت کا بھی خیال رکھیں۔ اپنی چیٹ ایپس میں حساس گفتگو کو باقاعدگی سے حذف کرنا اور اپنے براؤزنگ ہسٹری کو اپنے براؤزر ایپس سے حذف کرنا ایک اچھا عمل ہے۔

  - پہاڑی اور شہری محاذ کے ساتھیوں کو پہلے ہی میڈیا کے حوالے سے ہدایت نامہ جاری کیا جا چکا ہے۔

- **ایپل بیک اپ:**

کبھی بھی اپنے ڈیٹا کا iCloud میں بیک اپ نہ لیں۔ گو کہ Apple آپ کو بتائے گا کہ وہاں کا ڈیٹا انکرپٹڈ ہے، لیکن ان کے پاس خفیہ کاری کی چابیاں ہیں، اور مجرمانہ تفتیش کی صورت میں دائرہ اختیار کی تعمیل کرنے کا پابند ہے۔ اس وجہ سے بیک اپ کرنے سے مکمل طور پر گریز کرنا چاہئے.

- **اینڈرائیڈ بیک اپ:**

اینڈرائیڈ ڈیوائسز کو مختلف طریقوں سے ریموٹ بیک اپ کے ساتھ ہم آہنگ کیا جاتا ہے۔ سب کو غیر فعال کر دینا چاہیے۔

- **میموری کارڈز:**

بہت سے اینڈرائیڈ فونز میں مائیکرو ایس ڈی کارڈ ہوتے ہیں اور کچھ میں مائیکرو ایس ڈی کارڈز پہلے سے انسٹال ہوتے ہیں۔ یہ بہت خطرناک ہیں اور ان کا استعمال بالکل نہیں کرنا چاہیے۔ ایس ڈی کارڈ سے تصویر/ویڈیو/ڈیٹ فائل کو حذف کرنے کے بعد بھی انہیں مخصوص سافٹ ویئرز کے استعمال سے آسانی سے نکالا جا سکتا ہے۔ اس لیے، صرف اپنے موبائل فون کا اندرونی اسٹوریج استعمال کریں اور SD کارڈ ہٹا دیں۔

- **سوشل میڈیا کا استعمال:**

ہم محاذ جنگ پر موجود ساتھیوں کے لیے سوشل میڈیا کے استعمال کی حوصلہ شکنی کرتے ہیں۔ سوشل میڈیا، جیسے فیس بک، ٹویٹر، انسٹاگرام، سنیپ چیٹ، اور اسی

طرح کے دوسرے پلیٹ فارمز آپ کی سرگرمیوں کے بارے میں معلومات کا ذخیرہ نکال سکتے ہیں/مانیٹر کر سکتے ہیں۔ مثال کے طور پر فیس بک آپ کے آلے تک مکمل رسائی اور کنٹرول حاصل کرنا چاہتا ہے۔ اس کا دعویٰ ہے کہ یہ ایپ کی فعالیت کے لیے ضروری ہے۔ اسی طرح، فیس بک میسنجر آپکی نجی پیغامات کے لیے اینڈ ٹو اینڈ انکرپشن کا استعمال کرتا ہے، جو ممکنہ طور پر انکے سرور زپر plain text کے طور پر محفوظ رہتے ہیں۔ ان دوستوں کے لیے جنہیں اپنی تنظیمی ذمہ داریوں کی وجہ سے سوشل میڈیا کے استعمال کی ضرورت ہے وہ درج ذیل مراحل پر عمل کریں:

  - اپنا اصلی/پورا نام استعمال نہ کریں۔

- اپنے ذاتی ای میل ایڈریس سے علیحدہ ای میل ایڈریس کے ساتھ سائن اپ کریں۔
- ضرورت سے زیادہ معلومات فراہم نہ کریں۔
- ایسی پروفائل تصویر کا انتخاب کریں، جو آپ یا آپ کے مقام کی شناخت نہ کر پائے۔
- ایک مضبوط پاس ورڈ کا انتخاب کریں اور two-factor authentication کی توثیق کو فعال کریں۔
- پاس ورڈ کی بازیابی کے حصوں کے لیے غلط جوابات کا انتخاب کریں۔

- **انٹرنیٹ پر تلاش کرنا:**

گوگل کو تلاش کے لیے استعمال نہ کیا کریں کیونکہ یہ آپ کی تمام تلاشوں کا ریکارڈ رکھتا ہے اور آپکے آئی پی ایڈریس وغیرہ سمیت بہت سے دوسرے ڈیٹا کے ساتھ۔ ایک اچھا متبادل duckduckgo.com ہے، جو محفوظ ہے۔

- **لنکس پر کلک کرتے وقت محتاط رہیں:**

بہت سے ساتھیوں کے فون پر نادانستہ طور پر malware اور hacking software انسٹال ہو جاتے ہیں، کیونکہ انہوں نے کسی غیر شناسہ لنک پر کلک کیا ہوتا ہے۔ اجنبیوں کی طرف سے بھیجے گئے لنکس پر ہر گز کلک نہ کریں، یہاں تک کہ اگر وہ آپ کے ساتھیوں کے ذریعے بھیجے گئے ہیں، پھر بھی اس پر کلک کرنے سے پہلے لنک کی تصدیق کریں۔ کسی لنک میں ایڈریس پر جانے سے پہلے اسے باریکی سے دیکھیں۔

- **Attachments کھولتے وقت احتیاط برتیں:**

ایسے غیر متوقع فائلوں سے ہوشیار رہیں، جو ای میل، چیٹ، آواز یا دیگر پیغامات سے منسلک ہیں۔ یقینی بنائیں کہ بھیجنے والا وہی ہے جو آپ کے خیال میں ہے۔ ان سے دوسرے طریقے سے رابطہ کرنے کی کوشش کریں (مثال کے طور پر روبرو، یا فون کے ذریعے تصدیق کریں کہ آیا انہوں نے آپ کو ای میل بھیجا ہے)۔

(اختتام)

BALOCH LIBERATION ARMY

B.L.A

STRUGGLE TILL VICTORY